AF
IFW

PTO/SB/21 (12-97)
Approved for use through 9/30/00. OMB 0651-0031
Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paper Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

# TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

| | |
|---|---|
| Application Number | 09/406,910 |
| Filing Date | September 24, 1999 |
| In re Application of: | David S. HAYES |
| Group Art Unit | 2131 |
| Examiner Name | Zia, Syed |
| Customer No. | 25537 |
| Client Docket Number | RIC98054 |
| Total Number of Pages in This Submission | 24 |

## ENCLOSURES *(check all that apply)*

- ☒ Fee Transmittal Form
  - □ Fee Attached
- □ Amendment / Response
  - □ After Final
  - □ Affidavits/declaration(s)
- □ Extension of Time Request
- □ Express Abandonment Request
- □ Information Disclosure Statement
- □ Certified Copy of Priority Document(s)
- □ Response to Missing Parts/ Incomplete Application
  - □ Response to Missing Parts under 37 CFR 1.52 or 1.53
- □ Assignment Papers *(for an Application)*
- □ Drawing(s)
- □ Licensing-related Papers
- □ Petition Routing Slip (PTO/SB/69) and Accompanying Petition
- □ To Convert a Provisional Application
- □ Power of Attorney, Revocation Change of Correspondence Address
- □ Terminal Disclaimer
- □ Small Entity Statement
- □ Request of Refund
- □ After Allowance Communication to Group
- □ Appeal Communication to Board of Appeals and Interferences
- ☒ Appeal Communication to Group *(Appeal Notice, Brief, Reply Brief)*
- □ Proprietary Information
- □ Status Letter
- □ Additional Enclosure(s) *(please identify below)*:

Remarks: Revised Appeal Brief

## SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

| | |
|---|---|
| Firm or Individual name | DITTHAVONG & CARLSON, P.C.<br>Margo Livesay, Ph.D. , Reg. No. 41,946 |
| Signature | Margo Livesay |
| Date | November 23, 2005 |

## CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Assistant Commissioner for Patents, Alexandria, VA 22313-1450 on this date:

| | | | |
|---|---|---|---|
| Type or printed name | Margo Livesay, Ph.D. | | |
| Signature | Margo Livesay | Date | November 23, 2005 |

Burden Hour Statement: This form is estimated to take 0.2 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time your are required to complete this form should be sent to the Chief Information Officer, Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**
**BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES**

| | | | |
|---|---|---|---|
| In re Application of: | | | |
| | David S. HAYES | Conf. No.: | 2067 |
| Application No.: | 09/406,910 | Group Art Unit: | 2131 |
| Filed: | September 24, 1999 | Examiner: | Zia, Syed |
| Customer No.: | 25537 | | |
| Attorney Docket: | RIC 98 054 | | |
| Client Docket: | 09710-1202 | | |

For: METHOD FOR REAL-TIME DATA AUTHENTICATION

# REVISED APPEAL BRIEF

Honorable Commissioner for Patents
Alexandria, VA 22313-1450

Dear Sir:

This Appeal Brief is submitted in support of the Notice of Appeal dated June 6, 2005, and in response to the Notification of Non-Compliant Appeal Brief dated October 25, 2005.

## I. REAL PARTY IN INTEREST

MCI, Inc. is the real party in interest.

## II. RELATED APPEALS AND INTERFERENCES

Appellants are unaware of any related appeals and interferences.

## III. STATUS OF THE CLAIMS

Claims 1-17 are pending in this appeal. No claim is allowed. This appeal is therefore taken from the final rejection of claims 1-17 on March 9, 2005.

## IV. STATUS OF AMENDMENTS

The amendment to claims 1 and 13-17 filed May 9, 2005 has been entered and is relied upon in this appeal.

## V. SUMMARY OF THE CLAIMED SUBJECT MATTER

The present invention addresses problems associated with real-time data authentication utilizing a combination of public-key cryptography and digital signatures. (*See, e.g.*, specification, p. 1, ll. 6-8)

Public-key cryptography has traditionally been used to ensure the integrity of data. Used properly however, encryption may also be used to identify the source of the data, which may be important even when the data itself is not private. Thus, public key cryptography may be used to identify the source of the data by verifying that the data came from a source specifically identified by the private key. In this regard, the data is said to be signed, that is, affixed with a digital signature created only by the holder of a private key. Anyone who knows the corresponding public key can verify the digital signature. This assures that the data did in fact come from the person who holds the private key, and that the data has not been altered. (*See, e.g.*, specification, p. 1, l. 31 – p. 2, l. 3)

Although a digital signature assures the integrity of the data, it does not assure the identity of the sender. The receiver knows only that the data was signed by the holder of the private key, but they cannot be assured that any particular person is the holder of that key. Anyone could have generated a key pair, and attached the name of some other party to that key pair. This inability to reliably associate a real human being with a key pair is known as the "trust problem."

To address the trust problem, digital signatures are often used in conjunction with public-key certificates, or simply certificates. A certificate includes an identification of a keyholder (such as a name, address, phone number, or e-mail address), a copy of the public portion of the keyholder's key pair, and a digital signature from a third party certificate authority. The certificate authority functions as a sort of digital notary, attesting by its signature in the certificate that the keyholder identified is the real holder of the key pair given. Thus, the receiver need no longer trust the identity proclaimed by the sender's certificate. The receiver can rely on the certificate authority's signature incorporated into the sender's certificate, attesting to the sender's identity.

In addition to privacy and trust issues, other issues involve computing time and ease of implementation and use. (*See, e.g.,* specification, p. 2, l. 24 – p. 3, l. 10)

In accordance with a first aspect, a method is provided for authenticating transmitted data in real time, the method comprising the steps of generating a master cryptographic key pair, including a first public key and a first private key, publishing a first certificate issued by a certificate authority, the first certificate including the first public key and a first digital signature based on the first public key, generating a disposable cryptographic key pair, including a second public key and second private key, generating a second certificate, the second certificate including the second public key and a second digital signature based on the second public key, publishing the second certificate, signing the data to be transmitted with a third digital signature by processing the data to be transmitted through a one way hashing function to generate a first hash value and encrypting the first hash value utilizing the second private key, processing received data through the first one way hashing function to create a second hash value, decrypting the received third digital signature utilizing the second public key to obtain a third hash value, and verifying authenticity of the data by comparing the second hash value to the third hash value. (*See, e.g.,* specification, p. 4, ll. 13-25, claim 1)

In accordance with another aspect, a method is provided for digitally signing data in real time, comprising the steps of generating a master key pair including a first public key and a first private key, publishing a first certificate, the first certificate including the first public key and a first digital signature based on a key pair of a certificate authority, generating a disposable key pair, the disposable key pair including a second public key and a second private key, and wherein the disposable key pair is shorter than the master key pair, generating a second certificate, the second certificate including the second public key and a second digital signature based on the master key pair, dividing the data to be signed into the packets, for each packet of data, computing a hash value based on the data in the packet utilizing a one way hashing function, encrypting the hash value utilizing the second private key as the encryption key, and coupling each encrypted hash value with its corresponding data packet. (*See, e.g.,* specification, p. 4, l. 26 – p. 5, l. 2, claim 13)

In accordance with yet another aspect, a method is provided for verifying digitally signed data in real time, the method comprising the steps of processing a data portion of the digitally signed data through a one way hashing function to obtain a first hash value for each of the packets of digitally signed data, verifying contents of a first certificate issued by a certificate authority utilizing a public key issued by the certificate authority, the first certificate including a first public key of a long master key pair, verifying contents of a second certificate issued by a sender of the data utilizing the first public key from the first certificate, the second certificate including a second public key of a short disposable key pair, decrypting a digital signature portion of the digitally signed data utilizing the second public key to obtain a second hash value, and comparing the first and second hash values. (*See, e.g.,* specification, p. 5, ll. 3-12, claim 14)

In accordance with another aspect, a method is provided for digitally signing data in real time, the method comprising the steps of generating a disposable key pair, the disposable key pair including a short public key and a short private key, publishing the short public key, dividing data to be signed into the packets, for each packet of data, computing a hash value based on the data in the data packet utilizing a one way hashing function, encrypting the hash value utilizing the short private key, and coupling each encrypted hash value with its corresponding data packet. (*See, e.g.,* specification, p. 5, ll. 13-19, claim 15)

In accordance with another aspect, a method is provided for verifying digitally signed data in real time, the method comprising the steps of processing a data portion of the digitally signed data through a one way hashing function to obtain a first hash value for each of the packets of digitally signed data, decrypting a digital signature portion of the digitally signed data utilizing a published short public key to obtain a second hash value, and comparing the first and second hash values. (*See, e.g.,* specification, p. 5, ll. 20-25, claim 16)

Thus, exemplary methods and systems consistent with the present invention include simple to implement, effective and efficient methods and systems to authenticate digital data in real time utilizing a combination of cryptographic key pairs, disposable key pairs that are limited in size and duration, hashing functions, weak hashing functions to increase computational speeds, certificates from certificate authorities and self generated certificates. A method consistent with the present invention utilizes a series of certificates and digital signatures to serve as a mark of authenticity assuring the recipient that the data did in fact originate from an indicated source. The first certificate comprises the information used to decrypt and verify the information in the second certificate and is signed. The second certificate, which is also signed, comprises the information used to decrypt and verify the actual data. The data may be packetized and each packet is digitally signed utilizing a weak hashing function and short public key to decrease computational time. At the receiver's end, the digital signature is decoded to authenticate the data. Since the data itself is not encrypted, a receiver may utilize the data even though it is not verified. (*See, e.g.,* specification, p. 5, l. 26 – p. 6, l. 4) While the first certificate comprises a public key which is robust, the second certificate utilizes a smaller, less robust public key, thereby increasing the computational speed for real-time authentication. (*See, e.g.,* specification, p. 6, ll. 27-32, *see also* p. 7, ll. 1-4, claims 1, 13-17)

A sender desires to transmit data and wants the receiver to be able to authenticate the data in real time. The data to be transmitted may be any type of digital data, for example, digital video or digital audio. In addition, the method for real time data authentication may be utilized in conjunction with any type of transmission medium, for example, land line or wireless. As an example, the sender may be a television station and the receiver may be anyone tuned to that particular station. (*See, e.g.,* specification, p. 6, l. 33 – p. 7, l. 4, *see also* p. 12, l. 1 – p. 14, l. 25, Figure 5, claims 1, 13-17)

Figure 1 is a flow chart 100 setting forth steps of an exemplary method for real time authentication consistent with the present claimed invention. A sender generates a master cryptographic key pair comprising a first public key and a first private key (step 102). The master key pair may comprise any suitably long public and private keys sufficient to prevent individuals from decrypting any encrypted data in a reasonably short period of time. In step 104, the sender publishes a first certificate, which is issued by a certificate authority. The first certificate comprises an identification of the sender, an identification of the certificate authority, a copy of the first public key of the master cryptographic key pair generated by the sender, and a cryptographic check sum. The cryptographic check sum is an encrypted hash or digital signature. (*See, e.g.,* specification, p. 7, ll. 5-33, claim 1)

Figure 2 depicts a flow chart 200 of an exemplary method for generating a digital signature for the information in the first certificate and then verifying the information utilizing the signature. The data representing the identification of the sender, the identification of the certificate authority and the first public key is processed utilizing a one-way hashing function which generates a fixed size output (step 202) (*see, e.g.,* claim 1). In step 204, the fixed size hash value is encrypted, e.g., utilizing a private key from a cryptographic key pair generated by the certificate authority. The digital signature along with its associated data or information is transmitted at step 206, for example, as a television program. At step 208, the digital signature portion of the transmission is decrypted utilizing the certificate authority's public key thereby creating a decrypted hash value. The data portion of the transmission is processed utilizing the same one-way hash function as represented at step 202, in step 210, to create a fixed size hash value. The fixed size hash value and the decrypted hash value are compared. (*See, e.g.,* specification, p. 8, ll. 5-30, claim 1)

A disposable cryptographic key pair comprising a second public key and a second private key is generated as step 106 as shown in Figure 1. The disposable cryptographic key pair is much shorter than the master key pair so as to reduce computation time. In addition, the disposable cryptographic key pair may be utilized once and then discarded. Thus, methods consistent with the present invention utilize multiple cryptographic key pairs. (*See, e.g.,* specification, p. 8, l. 32 – p. 9, l. 5, claims 1, 13-17)

At step 108, the sender generates and publishes a second certificate comprising a second identification of the sender, an identification of the signing authority, a copy of the second public key, and a cryptographic check sum or digital signature. The second certificate is issued by the sender, and is published as widely as possible. The identification of the signing authority is the issuer of the certificate, which in this case is the sender. The second public key is part of the disposable cryptographic key pair generated by the sender. The digital signature in this second certificate is generated by the sender, and is utilized to ensure the integrity of the other data in the second certificate. (*See, e.g.,* specification, p. 9, ll. 6-19, claims 1, 13-17)

Figure 3 depicts a flowchart 300 of an exemplary method for generating a digital signature for the information in the second certificate and then verifying the information utilizing the signature. At step 302, the data representing the second identification of the sender, the identification of the signing authority, and the second public key is processed utilizing a one-way hashing function which generates a fixed size output. The fixed size hash value is then encrypted at step 304, for example, utilizing the first private key from the master key pair. Therefore, the encrypted hash value or digital signature may only be verified utilizing the first public key from the master key pair. The first public key from the master key pair is presumed to have been widely distributed or published and thus readily available. The digital signature along with its associated data is transmitted to a receiver at step 306. At step 308, the digital signature portion of the transmission is decrypted utilizing the master cryptographic key pair's first public key thereby creating a decrypted hash value. The data portion of the transmission is processed utilizing the same one-way hashing function as step 302, in step 310, to create a fixed size hash value. This fixed size hash value is compared to the decrypted hash value from step 308 at step 312. If the hash values match, then the data transmitted is valid. (*See, e.g.,* claims 1, 13-17)

Since it is assumed that the data or information comprising the first and second certificates is authentic, the receiver has a reliable copy of the first public key of the master cryptographic key pair and the second public key of the disposable cryptographic key pair. Accordingly, the sender may now transmit the data comprising the information to be shared with the receiver. (*See, e.g.,* specification, p. 9, l. 20 – p. 10, l. 14)

When data is packetized, each packet of data may be individually authenticated. For the transmission of data, each packet of data is signed as discussed above and the encryption is done with the second private key of the disposable cryptographic key pair (utilized because it is purposefully short and requires less computation time). A weaker hashing function may also be utilized at this point. (*See, e.g.,* claims 1, 13-17)

Each packet of data is protected by an encrypted hash or digital signature. For efficiency sake, a full certificate is not replicated in each data packet, rather just the data comprising each packet and the digital signature. (*See, e.g.,* specification, p. 10, ll. 16-26, claims 1, 13-17)

Figure 4 depicts a flowchart of an exemplary method for generating a digital signature for the data to be transmitted and then verifying the data utilizing the digital signature. At step 402, the data in the data packet is processed utilizing a one-way hashing function which generates a fixed size output. (*See, e.g.,* claims 13, 14) This hashing function may be much simpler than those previously described because the information used to verify the actual data was transmitted in the first and second certificates which utilized robust hashing functions. The fixed size hash value is then encrypted, for example, utilizing the second private key from the disposable cryptographic key pair, at step 404 (saving computation time by using the disposable cryptographic key pair which is intentionally made shorter than the master cryptographic key pair). (*See, e.g.,* claim 13) The digital signature along with the packet of data is transmitted at step 406. The digital signature portion is decrypted at step 408 utilizing the second public key of the disposable cryptographic key pair which was transmitted previously with the second certificate thereby creating a decrypted hash value. (*See, e.g.,* claim 14) The data portion is processed utilizing the same one-way hashing function as at step 402, in step 410, to create a fixed size hash value. If the two values match, then the data is authentic. (*See, e.g.,* claims 14, 17)

According to the present invention, it is the hash value that is encrypted and not the data itself. (*See, e.g.,* claims 1, 13-17) Accordingly, the data is not concealed or corrupted in any way. Even if a receiver were not able to authenticate the data, the receiver would still be able to view and utilize the data if he/she so desires. As each unit of signed data is received, the receiver strips off the digital signature for authentication and utilizes the data. The data may be read or otherwise utilized even without knowledge of the keys transmitted with the certificates, but only a recipient having the proper second public key can verify that the digital signature does indeed belong to the sender. All that is needed to utilize the data is to know the length of the digital signature so that the data portion can be stripped out. (*See, e.g.;,* specification, p. 10, l. 27 – p. 11, l. 22)

In accordance with the exemplary embodiment, the sender periodically retransmits the second certificate comprising the second public key. This is done because the receiver may have tuned into the transmission prior to receiving the second certificate and have no way of decrypting the digital signature. The periodic retransmission is interlaced with the signed data and may not interfere with the transmission. (*See, e.g.,* specification, p. 11, ll. 25-29)

These techniques may be advantageously used, for example, in Global Positioning Satellite systems (s*ee, e.g.,* specification, p. 12, l. 4), in telemedicine (s*ee, e.g.,* specification, p.

13, l. 27), in surveillance (*see, e.g.,* specification, p. 13, l. 34), or any digital network that relies on transmitting over the network control messages mixed with data (*see, e.g.,* specification, p. 14, ll. 13-14, claims 1, 13-17).

## VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Whether claims 1-17 are anticipated under 35 U.S.C § 102(b) by *Matyas et al.* (US 5,200,999).

## VII. ARGUMENT

### A. CLAIMS 1-17 ARE NOT ANTICIPATED OVER *MATYAS ET AL.*

To anticipate a patent claim, every element and limitation of the claimed invention must be found in a single prior art reference, arranged as in the claim. *Karsten Mfg. Corp. v. Cleveland Golf Co.*, 242 F.3d 1376, 1383, 58 USPQ2d 1286, 1291 (Fed. Cir. 2001); *Scripps Clinic & Research Foundation v. Genentech, Inc.*, 927 F.2d 1565, 1576, 18 USPQ2d 1001, 1010 (Fed. Cir. 1991).

A prior art reference anticipates a patent claim if it discloses every limitation of the claimed invention, either explicitly or inherently. *In re Schreiber*, 128 F.3d 1473, 1477, 44 USPQ2d 1429, 1431 (Fed. Cir. 1997). "Under the principles of inherency, if the prior art necessarily functions in accordance with, or includes, the claimed limitations, it anticipates." *MEHL/Biophile Int'l Corp. v. Milgraum*, 192 F.3d 1362, 1365, 52 USPQ2d 1303, 1305 (Fed. Cir. 1999).

Unless the patent otherwise provides, a claim term cannot be given a different meaning in the various claims of the same patent. *Georgia Pacific Corp. v. U.S. Gypsum Co.,* 195 F.3d 1322, 1331, 52 USPQ2d 1590, 1598 (Fed. Cir., Nov. 1, 1999); see also *Southwall Tech., Inc. v.*

*Cardinal IG Co.*, 54 F.3d 1570, 1579, 34 USPQ2d 1673, 1679 (Fed. Cir. 1995) (holding that claim term found in different claims must be interpreted consistently); *Fonar Corp. v. Johnson & Johnson*, 821 F.2d 627, 632, 3 USPQ2d 1109, 1113 (Fed. Cir. 1987.) (holding that a term used in one claim had the same meaning in another claim).

Well-settled case law holds that the words of a claim must be read as they would be interpreted by those of ordinary skill in the art. *In re Baker Hughes Inc.,* 215 F.3d 1297, 55 USPQ2d 1149 (Fed. Cir. 2000); *In re Morris*, 127 F.3d 1048, 1054, 44 USPQ2d 1023, 1027 (Fed. Cir. 1997); M.P.E.P. 2111.01. "Although the PTO must give claims their broadest reasonable interpretation, this interpretation must be consistent with the one that those skilled in the art would reach." *In re Cortright,* 165 F.3d 1353, 1369, 49 USPQ2d 1464, 1465 (Fed. Cir. 1999).

### 1. CLAIMS 1-17 ARE NOT ANTICIPATED BY *MATYAS ET AL.* BECAUSE *MATYAS ET AL.* DOES NOT DISLCOSE "TRANSMITTED AS A STREAM OF PACKETS OVER A PUBLICLY AVAILABLE MEDIUM."

The rejection of claims 1-17 must be reversed, because *Matyas et al.* does not disclose the limitations of the claims.

*Matyas et al.* (Per Abstract) is directed to a data processing system, method and program for managing a public key cryptographic system. The method includes the steps of generating a first public key and a first private key as a first pair in the data processing system, for use with a first public key algorithm and further generating a second public key and a second private key as a second pair, for use with a second public key algorithm. The method then assigns a private control vector for the first private key and the second private key, for defining permitted uses for the first and second private keys. A private key record is formed which includes the first private key and the second private key, and the private key record is encrypted under a first master key expression which is a function of the private control vector. A private key token is formed which includes the private control vector and the private key record, and the private key token is stored in the data processing system. At a later time, the method receives a first key use request, requiring the first public key algorithm. In response to this, the private key token is accessed and the private control vector is checked to determine if the private key record contains a key having permitted uses which will satisfy the first request. The method then decrypts the private key record under the first master key expression and extracts the first private key from the private key record. The method selects the first public key algorithm for the first key use request and executes the first public key algorithm using the first private key to perform a cryptographic operation to satisfy the first key use request.

The preambles of claims 1 and 13-17 of the present application clearly specify that the data was or is to "transmitted as a stream of packets over a publicly available medium." *Matyas et al.* does not disclose this feature; the portion cited by the Examiner (Office Action dated March 9, 2005, p. 9), col. 9: 35-54, in conjunction with claim 12 merely mentions a "general method for control." Thus, the rejections of independent claims 1 and 13-17, and dependent claims 2-12, should be reversed.

## 2. CLAIMS 1-12 ARE NOT ANTICIPATED BY *MATYAS ET AL.*

Furthermore, independent claim 1 recites, and dependent claims 2-12 incorporate pursuant to 35 U.S.C. § 112, ¶ 4, three different digital signatures of three different **contents** (in **bold**) with three different *private keys* (in *italics*):

> 1. (Previously Presented) A method for authenticating transmitted data in real time, the method comprising the steps of:
>
> (a) generating a master cryptographic key pair, including a first public key and a first private key;

(b) publishing a first certificate issued by a certificate authority, the first certificate including the first public key and **a first digital signature of the first public key** *based on a private key from the certificate authority*;
(c) generating a disposable cryptographic key pair, including a second public key and second private key;
(d) generating a second certificate, the second certificate including the second public key and **a second digital signature of the second public key** *based on the first private key*;
(e) publishing the second certificate;
(f) **signing data to be transmitted with a third digital signature** by processing the data to be transmitted through a first one way hashing function to generate a first hash value and encrypting the first hash value *utilizing the second private key*;
(g) processing received data through the first one way hashing function to create a second hash value;
(h) decrypting the received third digital signature utilizing the second public key to obtain a third hash value; and
(i) verifying authenticity of the received data by comparing the second hash value to the third hash value,
wherein the first private key, the second private key, and the private key from the certificate authority have different values.

This feature is not shown in *Matyas et al. Matyas et al.* merely mentions a PR2 master key "used to generate an authentication signature for the public and private keys kept outside the cryptographic facility" (col. 9: 47-50), but *Matyas et al.* fails to describe a system with "a first digital signature of **the first public key** based on *a private key from the certificate authority*" and "a second digital signature of **the second public key** based on *the first private key*" in which "wherein the first private key, the second private key, and the private key from the certificate authority have different values" as recited in claim 1. In fact, *Matyas et al.* does not even describe digital signatures "based on a private key from the certificate authority."

The passages of *Matyas et al.* cited by the Examiner (Office Action dated March 9, 2005, pp. 4-5), namely cols. 12: 28– col. 13: 9, col. 24: 43– col. 26: 14, col. 68: 15-55, and col. 129: 4-14, do not support the rejection because there is no description there of a digital signature for a public key, much less any digital signatures of public keys based on private keys from any certificate authority. Thus the rejection of claims 1-12 should be reversed.

### 3. CLAIM 13 IS NOT ANTICIPATED BY *MATYAS ET AL.*

Furthermore, independent claim 13 recites:

> (b) publishing a first certificate, the first certificate including the first public key and a first digital signature based on *a key pair of a certificate authority*;
> (c) generating a disposable key pair, the disposable key pair including a second public key and a second private key, and **wherein the disposable key pair is shorter than the master key pair**;
> (d) generating a second certificate, the second certificate including the second public key and a second digital signature *based on the master key pair*;
> (g) encrypting the hash value utilizing the *second private key* as the encryption key; and

*Matyas et al.* does not disclose this feature because only the PR2 master key is used to generate signatures in the *Matyas et al.* system, and there is no disclosure of any "disposable key pair" used to generate the recited second digital signature in *Matyas et al.* that is "shorter than" the PR2 master key. Thus, the rejection of claim 13 should be reversed.

### 4. CLAIMS 14-16 ARE NOT ANTICIPATED BY *MATYAS ET AL.*

For reasons similar to those discussed previously, independent claim 15, which recites "a digital signature of the short public key based on a long private key longer than the short private key," is also patentable over *Matyas et al.*—as are independent claim 14 ("a short disposable key pair that is shorter than the long master key pair") and independent claim 16 ("wherein the short public key is shorter than the long public key"). Thus, the rejections of claims 14-16 should be reversed.

### 5. CLAIM 17 IS NOT ANTICIPATED BY *MATYAS ET AL.*

Independent claim 17 sets forth "verifying the first public key based on a digital signature of a second public key issued by a certificate authority and having a different value than the first public key." For the reasons described above, nothing in *Matyas et al.*, including the PR2 master key, satisfies this feature, and thus the rejection of claim 17 should be reversed.

## VIII. CONCLUSION AND PRAYER FOR RELIEF

For the foregoing reasons, Appellant requests the Honorable Board to reverse each of the Examiner's rejections.

Respectfully Submitted,

DITTHAVONG & CARLSON, P.C.

November 23 2005
Date

Margo Livesay
Margo Livesay, Ph.D.
Attorney for Applicant(s)
Reg. No. 41,946

10507 Braddock Rd, Suite A
Fairfax, VA 22032
Tel. 703-425-8501
Fax. 703-425-8518

## IX. CLAIMS APPENDIX

1. (Previously Presented) A method for authenticating transmitted data in real time, said data transmitted as a stream of packets over a publicly available medium, the method comprising the steps of:

(a) generating a master cryptographic key pair, including a first public key and a first private key;

(b) publishing a first certificate issued by a certificate authority, the first certificate including the first public key and a first digital signature of the first public key based on a private key from the certificate authority;

(c) generating a disposable cryptographic key pair, including a second public key and second private key;

(d) generating a second certificate, the second certificate including the second public key and a second digital signature of the second public key based on the first private key;

(e) publishing the second certificate;

(f) signing the packets of data to be transmitted with a third digital signature by processing the data to be transmitted through a first one way hashing function to generate a first hash value and encrypting the first hash value utilizing the second private key;

(g) processing received data through the first one way hashing function to create a second hash value;

(h) decrypting the received third digital signature utilizing the second public key to obtain a third hash value; and

(i) verifying authenticity of the received data by comparing the second hash value to the third hash value,

wherein the first private key, the second private key, and the private key from the certificate authority have different values.

2. (Original) The method for authenticating transmitted data in real time according to claim 1, wherein the step of generating a master key pair comprises creating long first public and private keys.

3. (Previously Presented) The method for authenticating transmitted data in real time according to claim 1, wherein the first certificate further includes an identification of a sender and an identification of a certificate authority issuing the first certificate.

4. (Previously Presented) The method for authenticating transmitted data in real time according to claim 3, wherein the first digital signature is produced by:

(a) processing information representing the identification of the sender, the identification of the certificate authority issuing the first certificate and the first public key through a second one way hashing function to create a fourth hash value; and

(b) encrypting the fourth hash value utilizing the private key from the certificate authority issuing the first certificate to create the first digital signature.

5. (Previously Presented) The method for authenticating transmitted data in real time according to claim 4, further comprising the step of verifying authenticity of data comprising the first certificate.

6. (Previously Presented) The method for authenticating transmitted data in real time according to claim 5, wherein the step of verifying the authenticity of the data comprising the first certificate comprises:

(a) decrypting the first digital signature to obtain a fifth hash value utilizing a public key issued by the certificate authority issuing the first certificate;

(b) processing the received information representing the identification of the sender, the identification of the certificate authority issuing the first certificate and the first public key through the second one way hashing function to create a sixth hash value; and

(c) comparing the fifth and sixth hash values.

7. (Original) The method for authenticating transmitted data in real time according to claim l, wherein the step of generating a disposable cryptographic key pair comprises generating short second public and private keys.

8. (Previously Presented) The method for authenticating transmitted data in real time according to claim l, wherein the second certificate further includes the identification of the sender and an identification of a signing authority issuing the second certificate.

9. (Previously Presented) The method for authenticating transmitted data in real time according to claim 8, wherein the second digital signature is produced by:

(a) processing the data representing the identification of the sender, the identification of the signing authority issuing the second certificate and the second public key through a third one way hashing function to create a seventh hash value; and

(b) encrypting the seventh hash value utilizing the first private key to create the second digital signature.

10. (Previously Presented) The method for authenticating transmitted data in real time according to claim 9, further comprising the step of verifying the authenticity of the data comprising the second certificate.

11. (Previously Presented) The method for authenticating transmitted data in real time according to claim 10, wherein the step of verifying the authenticity of the data comprising the second certificate comprises:

(a) decrypting the second digital signature to obtain an eighth hash value utilizing the first public key;

(b) processing the received data representing the identification of the sender, the identification of the signing authority issuing the second certificate and the second public key through the third one way hashing function to create a ninth hash value; and

(c) comparing the eighth and ninth hash values.

12. (Previously Presented) The method for authenticating transmitted data in real time according to claim 1, further comprising dividing the data into packets and signing and authenticating each packet of data in accordance with steps (f) through (i) of claim 1.

13. (Previously Presented) A method for digitally signing data in real time, said data to be transmitted as a stream of packets over a publicly available medium, the method comprising the steps of:

(a) generating a master key pair including a first public key and a first private key;

(b) publishing a first certificate, the first certificate including the first public key and a first digital signature based on a key pair of a certificate authority;

(c) generating a disposable key pair, the disposable key pair including a second public key and a second private key, and wherein the disposable key pair is shorter than the master key pair;

(d) generating a second certificate, the second certificate including the second public key and a second digital signature based on the master key pair;

(e) dividing the data to be signed into the packets;

(f) for each packet of data, computing a hash value based on the data in the packet utilizing a one way hashing function;

(g) encrypting the hash value utilizing the second private key as the encryption key; and

(h) coupling each encrypted hash value with its corresponding data packet.

14. (Previously Presented) A method for verifying digitally signed data in real time, said data transmitted as a stream of packets over a publicly available medium, the method comprising the steps of:

(a) processing a data portion of the digitally signed data through a one way hashing function to obtain a first hash value for each of the packets of digitally signed data;

(b) verifying contents of a first certificate issued by a certificate authority utilizing a public key issued by the certificate authority, the first certificate including a first public key of a long master key pair;

(c) verifying contents of a second certificate issued by a sender of the data utilizing the first public key from the first certificate, the second certificate including a second public key of a short disposable key pair that is shorter than the long master key pair;

(d) decrypting a digital signature portion of the digitally signed data utilizing the second public key to obtain a second hash value; and

(e) comparing the first and second hash values.

15. (Previously Presented) A method for digitally signing data in real time, said data to be transmitted as a stream of packets over a publicly available medium, the method comprising the steps of:

(a) generating a disposable key pair, the disposable key pair including a short public key and a short private key;

(b) publishing the short public key and a digital signature of the short public key based on a long private key longer than the short private key;

(c) dividing data to be signed into the packets;

(d) for each packet of data, computing a hash value based on the data in the data packet utilizing a one way hashing function;

(e) encrypting the hash value utilizing the short private key; and

(f) coupling each encrypted hash value with its corresponding data packet.

16. (Previously Presented) A method for verifying digitally signed data in real time, said data transmitted as a stream of packets over a publicly available medium, the method comprising the steps of:

(a) processing a data portion of the digitally signed data through a one way hashing function to obtain a first hash value for each of the packets of digitally signed data;

(b) decrypting a digital signature portion of the digitally signed data utilizing a published short public key to obtain a second hash value;

(c) comparing the first and second hash values; and

(d) verifying a digital signature of the short public key based on a long public key, wherein the short public key is shorter than the long public key.

17. (Previously Presented) A method for verifying digitally signed data in real time, said data transmitted as a stream of packets over a publicly available medium, the method comprising the steps of:

receiving one of the packets including an unencrypted data portion and a digital signature portion;

generating a first hash value by processing the received unencrypted data portion through a one way hashing function;

decrypting the received digital signature utilizing a first public key to obtain a second hash value;

verifying the digitally signed data by comparing the first hash value to the second hash value; and

verifying the first public key based on a digital signature of a second public key issued by a certificate authority and having a different value than the first public key.